

## **Requesting a Mainframe Logon ID**

### **Objective**

1. To obtain a mainframe logon ID for an employee who needs access to one or more of these systems: Minnesota Accounting and Procurement System (MAPS), Statewide Employee Management System (SEMA4), DocumentDirect, or InfoPac.
2. To resolve certain logon ID-related problems, such as forgotten passwords.

### **Policy**

Before an employee can be cleared to use MAPS, SEMA4, DocumentDirect, InfoPac, or any other system that runs on the mainframe computer operated by the Office of Enterprise Technology (OET), the employee must have a valid mainframe logon ID. A logon ID is a seven-character alphanumeric identification code. The first two characters of the logon ID are typically letters, and they stand for the agency for which the person works. The last five characters are typically a combination of letters and numbers.

The Office of Enterprise Technology is responsible for overseeing the logon ID database and establishing certain policies, including password policies.


Each employing agency is responsible for identifying employees who need mainframe logon ID's and taking appropriate action. Typically a large agency has in-house ACF2 (mainframe) security officers who have the power to create logon ID's. Every other agency has at least one person who is designated as a mainframe data security contact. This person is responsible for obtaining logon ID's for employees who need them by submitting requests to OET via OET's password-protected web request form.


With rare exceptions, each employee is entitled to a maximum of one logon ID. If an employee is already authorized to use one mainframe system and needs to be authorized to use an additional mainframe system, you should not request an additional logon ID. When completing a system access form to authorize the employee for the additional system, simply enter the current logon ID on the form.

**Forgotten passwords:** If a user of MAPS, SEMA4, DocumentDirect, or InfoPac forgets his/her password, the employee should follow his/her agency's internal policy, if any. If the agency does not have an internal policy for handling this problem, the user should call the Statewide Administrative Systems Help Line at (651) 201-8100 and select either the MAPS Security option or the SEMA4 Security option. If the user is authorized for DocumentDirect/InfoPac but not MAPS or SEMA4, he/she should select the MAPS Security option.

### **General Procedures**

<b>Step #</b>	<b>Actions to be Performed</b>	<b>Responsible Party</b>
1.	Determine whether employee already has a valid mainframe logon ID whose first two characters match	Agency, Supervisor

	<p>the standard for your agency. If so, do not request an additional logon ID. With rare exceptions, each user is entitled to only one. If the user has a valid logon ID, refer to the appropriate system-specific policy, such as <a href="#">1101-02, Requesting Basic Access to MAPS</a>.</p>	
2.	<p>Following your agency's internal policy, ask an authorized person to create a logon ID or submit a request to the Office of Enterprise Technology (OET).</p> <ul style="list-style-type: none"> <li>· If your agency has an ACF2 (mainframe) security officer (most large agencies do), ask the person to create a logon ID. Go to step 3.</li> <li>· If your agency does not have an ACF2 security officer, ask your agency's mainframe data security contact to submit a logon ID request via OET's password-protected web request form. Your agency might have several people who are designated as data security contacts. The primary data security contact might be someone in the information technology area, or the accounting director, or the head of the agency. Skip to step 4.</li> </ul> <p>Note: OET no longer accepts logon ID requests via mail, fax, or E-mail. The data security contact must use OET's web-based request form.</p>	Agency, Supervisor
3.	<p>Create a mainframe logon ID and an initial password. Skip to step 7.</p>	Agency, Security Officer
4.	<p>Go to OET's web site. (The following navigation instructions are subject to change at any time.) Go to <a href="http://www.oet.state.mn.us">www.oet.state.mn.us</a>. On the gray bar near the top, click on "Customers." Then click on "Quick Links for Customers," and finally, "Security ACF2 Request Form." When prompted to enter your user name and password, enter the user name that the Office of Enterprise Technology has assigned to you for this site. (It is unrelated to your mainframe logon ID, if any.) Also enter your current password for this site. If you have forgotten your user name and/or password for this site, send an E-mail to OET at:  <a href="#">data-</a></p>	Agency, Data Security Contact

	<a href="mailto:security@lists.state.mn.us">security@lists.state.mn.us</a> 	
5.	Fill in the Mainframe Logon ID Request screen and click on the Send button. Watch for an E-mail from OET within one or two working days.	Agency, Data Security Contact
6.	Create a mainframe logon ID and initial password. Send the data security contact an E-mail containing a service request number and a link to a page on the OET web site that shows the logon ID and password.	Office of Enterprise Technology
7.	Following your agency's internal policy, inform the supervisor and/or other appropriate personnel of the logon ID and inform someone, such as the supervisor and/or the user, of the initial password.	Agency, Security Officer or Data Security Contact
8.	<p>Advise the employee that upon signing on to the mainframe with the initial password, he/she must enter a new password in the proper fields. Inform the employee of the requirements regarding passwords. (Print a copy of this step and give it to the employee.) The new password must:</p> <ul style="list-style-type: none"> <li>· be exactly eight (8) characters long.</li> <li>· contain at least 1 letter. (Also, the MAPS software requires the first character of the password to be a letter. Mainframe passwords are not case-sensitive.)</li> <li>· contain at least 1 number.</li> <li>· contain at least 1 of the following special characters: * \$ : - ! . % ? @ # _ &amp; (The special character[s] cannot be the first or last character of the password.)</li> <li>· not contain 3 of the same character in a row. (Example: r@bbbit3 would not work, but r@bbit33 would work.)</li> </ul> <p>Also inform the employee of these time constraints:</p> <ul style="list-style-type: none"> <li>· A new password must be retained for a minimum of 5 days.</li> <li>· The password must be changed a minimum of every</li> </ul>	Agency, Supervisor or Other Personnel

	<p>30 days.</p> <ul style="list-style-type: none"> <li>· A previously used password cannot be reused for at least 6 password cycles.</li> </ul> <p>Note: The employee may change the initial password as soon as he/she receives it. If the employee uses the MAPS sign-on screen to change the password but he/she is not yet authorized to use MAPS, the mainframe will issue the message "Password successfully altered," and then MAPS will issue the message "Front end sign-on failed." The employee may ignore the second message. It is unrelated to the password.</p>	
9.	<p>If the employee needs access to MAPS, follow policy <a href="#">1101-02, Requesting Basic Access to MAPS</a>.</p>	Agency